

# IOT Scheme Study

---

**Authors: Internet of Trust S.A.S. (IOTR) – TÜV Informationstechnik GmbH (TÜViT)**

Release: 1.1 –Final report for Eurosmart members distribution

Date: 10/10/2019

## **Forward – Disclaimer**

The present report is based on data collected during the following period: May 19-Sept 19.

The content of this document does not reflect the official opinion of Eurosmart. This is intended for informative purposes only, Eurosmart is not liable for the accuracy of the information contained in this study.

## **Acknowledgement**

Internet of Trust and TÜViT would like address a warm thank you to all the people who accepted to spend time to fill the questionnaires. These contribution were essential to collect the information gathered in this report.

## Table of Contents

Table of Contents .....	2
List of Tables.....	3
1. Introduction.....	4
1.1. Objective.....	4
1.2. List of schemes .....	4
1.3. Content.....	5
1.4. Information Collection Method.....	5
2. Result Synthesis.....	6
2.1. Schemes Overview (Q3, Q5).....	6
2.2. Targeted Market and Users (Q1, Q2) .....	8
2.3. Operational Description and Governance of the Scheme (Q4, Q6, Q7, Q8, Q9, Q10, Q11, Q31, Q32, Q33, Q34).....	11
2.4. Products Evaluated by the Scheme (Q22, Q23, Q24).....	15
2.5. Evaluation Methodology/-ies used by each Scheme .....	17
2.5.1. Evaluation Labs (Q18, Q19, Q20, Q21).....	17
2.5.2. Evaluation Process (Q12, Q13, Q14, Q15, Q16, Q17).....	18
2.5.3. Testing Process (Q25, Q26, Q27, Q28, Q29, Q30).....	22
2.6. Compliance Level with Art. 54 of the Cyber Security Act (Q35).....	25
3. References.....	27
4. Revision History .....	30

## List of Tables

Table 1: Scheme overview (Q3, Q5)	6
Table 2: Targeted markets (Q1)	8
Table 3: Users of the schemes (Q2)	10
Table 4: Scheme details (Q4, Q6, Q7, Q8, Q9)	11
Table 5: Scheme maintenance (Q10, Q11)	13
Table 6: Risk Analysis and Management (Q31, Q32, Q33, Q34)	14
Table 7: Mapping between schemes and products (Q22, Q23, Q24)	15
Table 8: Evaluation Labs (Q18, Q19, Q20, Q21)	17
Table 9: Evaluation Process (Q12, Q13)	18
Table 10: Evaluation requirements (Q14, Q16)	19
Table 11: Supporting documents of the schemes (Q17)	21
Table 12: Compliance overview (Q25, Q26, Q27, Q28, Q29, Q30)	22
Table 13: Compliance overview (Q35)	25
Table 14: Compliance details	26

# I. Introduction

## I.1. Objective

The work consists in a study of 18 IoT certification schemes selected by Eurosmart that are applicable in Europe. This study provides an overview of the studied schemes on various criteria. It aims at providing a common understanding of the main targeted product or group of products, the associated markets and users, the technical characteristics, and the potential compliance with the European Cybersecurity Certification framework. This report represents a summary of the details provided in questionnaires filled in by contacts identified by Eurosmart for each scheme.

Part of this study are the following documents:

- The questionnaire template which has been provided to collect information for each scheme,
- 16 questionnaires filled in by people who are familiar with the respective scheme,
- An excel sheet to provide an overview of certification bodies and evaluation labs for each scheme,
- This summary report.

## I.2. List of schemes

The following IoT certification schemes have been chosen:

1. Eurosmart IoTSCS
2. ARM PSA
3. SESIP
4. UL IoT Security Rating
5. UL 2900
6. UL IEC 62443
7. CSPN (ANSSI)
8. Baseline certification (BSI)
9. BSPA (NCSA)
10. LINCE (CCN)
11. SOG-IS for IoT
12. Global Platform TEE
13. Global Platform SE
14. Commercial Product Assurance from CESG (UK)
15. ETSI TS103 655 – Cybersecurity for consumer IoT
16. IoT Security Foundation
17. GSMA
18. TÜViT-SQ Security Qualification

The first 15 were in Eurosmart initial list, 16 and 17 have been added by Eurosmart, 18 is proposed by TÜViT. Questionnaires for scheme 13 has been promised but not yet provided. Scheme 14 has been replaced by the Commercial Product Assurance led by the NCSC. For this scheme, information can be found online (<https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa>), however, no filled questionnaire has been provided. For Scheme 17, a questionnaire was sent to a contact identified by Eurosmart, however, no filled questionnaire has been provided.

Please further note that scheme 15 is actually no certification scheme. It is rather an industry standard.

### 1.3. Content

The questionnaire has been designed by Internet of Trust and TÜViT and validated by Eurosmart.

The responsibility of TÜViT and Internet of Trust is limited to the collection and the aggregation of the answers.

### 1.4. Information Collection Method

The followed method that has been conducted for information collection consists of the following steps:

1. Questionnaire sent by email to the point of contact communicated by Eurosmart.
2. For some schemes, a first interview is conducted in the aim of clarifying the scope of the study and explaining questions.
3. Reception of a first draft filled by the point of contact.
4. Review of the first draft by IOTR or TÜViT.
5. Interview with the contact point to complete the questionnaire (for some schemes, two interviews were needed to complete the questionnaire).
6. Following the interview, a final version for validation is provided to the point of contact.
7. Finally, the answers are added in the current document for analysis. Note that in case filled questionnaires have been available for the same scheme but from different people, the information provided has been merged.

## 2. Result Synthesis

### 2.1. Schemes Overview (Q3, Q5)

Table 1: Scheme overview (Q3, Q5)

Identifier	Description	Public or private scheme	Scheme owner	Launched	Number of received questionnaires	Participants (Questionnaire filled by)	Followed-up by
<b>BSPA (NLNCSA)</b>	The Dutch Scheme for Baseline Security Product Assessment	Public	AIVD/NLNCSA	2015	1	NLNCSA	Internet of Trust
<b>CSPN (ANSSI)</b>	French First Level Certification	Public	ANSSI	2008	2	ANSSI SRC	Internet of Trust
<b>Eurosmart IoTSCS</b>	Eurosmart own certification scheme for IoT devices with a focus on the Substantial security assurance level	Public	Eurosmart organisation	June 2019	2	Red Alert Lab Trusted Objects	Internet of Trust
<b>IoTSEF</b>	IoT Security Best Practice Guidelines for the design of connected consumer products	Public	IoT Security Foundation	2016	1	IoTSEF	Internet of Trust
<b>LINCE</b>	This methodology is designed for ICT products requiring certification with medium or low security criticality.	Public	CCN	June 2018	1	Applus	Internet of Trust
<b>PSA L1</b>	Security model based critical security questions with lab interview <ul style="list-style-type: none"> <li>For Chip vendors</li> <li>For OS suppliers</li> <li>For OEMs</li> </ul>	Private	PSA Joint Stakeholder Agreement Members	February 2019	2	Prove&Run Brightsight	Internet of Trust
<b>PSA L2</b>	Lab based evaluation of the PSA-RoT Mid assurance & mid robustness <ul style="list-style-type: none"> <li>For Chip Vendors</li> </ul>	Private	PSA Joint Stakeholder Agreement Members	February 2019	2	Prove&Run Brightsight	Internet of Trust
<b>UL IoT Security Rating</b>	UL's IoT Security Rating is a highly efficient and comprehensive evaluation process that assesses critical security aspects of smart products against common	Private	UL	May 2019	1	UL	Internet of Trust

Identifier	Description	Public or private scheme	Scheme owner	Launched	Number of received questionnaires	Participants (Questionnaire filled by)	Followed-up by
	attack methodologies and known IoT vulnerabilities, to create a 'security baseline' among the consumer IoT industry.						
<b>UL 2900</b>	UL 2900 is a series of standards published by UL (formerly Underwriters Laboratories), a global safety consulting and certification company. The standards present general software cyber security requirements for network-connectable products (UL 2900-1), as well as requirements specifically for medical and healthcare systems (UL 2900-2-1), industrial control systems (UL 2900-2-2), and security and life safety signaling systems (UL 2900-2-3).	Public	UL	2016: UL test outline 2017: ANSI standard	1	UL	Internet of Trust
<b>UL IEC 62443</b>	The IEC 62443 family of standards has cybersecurity requirements for industrial automation control systems that a manufacturer or system integrator needs to instill cybersecurity rigor into their processes.	Public	ISA	2018 / 2019	1	UL	Internet of Trust
<b>BSI Base Certification</b>	Security scheme like CSPN and BSPA	Public (not yet finalized)	BSI	Q4 2019	1	SRC	TÜVIT
<b>SOG-IS (CC)</b>	Common Criteria certification scheme	Public	SOG-IS	No answer provided.	1	SRC	TÜVIT
<b>SESIP</b>	The Security Evaluation Standard for IoT Platforms (SESIP) defines a standard for trustworthy assessment of the	Public	TrustCB, however, scheme is in a transition state to become an open standard.	December 2018	1	TrustCB	TÜVIT

Identifier	Description	Public or private scheme	Scheme owner	Launched	Number of received questionnaires	Participants (Questionnaire filled by)	Followed-up by
	security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains.						
<b>TÜVIT-SQ</b>	Security Qualification for trusted products and trusted sites	Private	TÜV Informationstechnik GmbH (TÜVIT)	Current version is 10.0 The scheme was launched more than 10 years ago	1	TÜVIT	TÜVIT
<b>ETSI</b>	European Telecommunications Standards Institute	Public	ETSI	No answer provided	1	Eurosmart	TÜVIT
<b>GP TEE</b>	Global Platform Trusted Execution Environment	Public	Global Platform	2015	1	Global Platform	TÜVIT
<b>GP SE</b>	Global Platform Secure Element		Global Platform				TÜVIT
<b>GSMA</b>	Global System for Mobile Communications		GSMA				TÜVIT
<b>CPA</b>	Commercial Product Assurance		NCSC				TÜVIT

## 2.2. Targeted Market and Users (Q1, Q2)

The following table provides an overview of the targeted markets of each scheme.

**Table 2: Targeted markets (Q1)**

List of targeted markets																				
	BSPA (NINCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA	
Automotive		x	x	x	x	x				x			x	x		x				
Energy metering		x	x	x	x	x	x	x	x			x	x			x				
Industry 4.0		x	x	x	x	x	x	x	x	x	x	x	x	x		x				
IoT Device (components of PCB)		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
Medical devices		x	x	x	x	x	x	x	x	x	x	x	x	x		x				



List of targeted markets	List of targeted markets																			
	BSPA (NINCSA)	CSPN (ANSSI)		IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Payment applications / online banking		x	x	x																
Connectivity (eUICC, network products)		x	x	x	x	x							x	x		x				
Government (Qscd, passport, ...)	x	x		x									x							
Access control	x	x		x	x	x	x	x	x				x	x	x		x			
Time stamping		x		x	x	x								x	x					
General purpose methodology (could be applicable for any markets)		x		x																
Other answers added by the scheme	(1)		(4)				(5)	(5)	(5)	(6)	(2)				(7)					

Please note that the last row 'General purpose methodology' was added by the authors of this document to summarize the different schemes addressed in this study.

Other answers:

- (1) Network Security, Network filtering, detection and response, secure messaging, Media and file security
- (2) Network Devices
- (3) Smart Home, Smart Cities, Smart health, Tracking system (vehicle), etc.
- (4) Consumer (smart home, consumer electronics, etc.), Enterprise (Businesses, Connected Schools, Smart Building, Financial Institutions, etc.)
- (5) Smart home, smart building and Industry 4.0/industrial IoT security standards or frameworks applicable at product-, system- and/or process-level.
- (6) Cross-sector: IoT-class component, device, product and service providers
- (7) The SQ based on TOE specific security requirements and is suitable for evaluation of a wide variety of IT systems/products.

The following table summarizes users of the scheme:

**Table 3: Users of the schemes (Q2)**

List of targeted markets																			
	BSPA (NLNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
List of developers and organizations that insist on products being certified based on the scheme																			
Chip manufacturers (Silicon and Firmware)	x	x	x	x	x	x					(13)		x	x	(14)	x			
OS Developers	x	x	x	x	x								x	x		x			
Application Developers	x	x	x	x	x								x	x		x			
Device Makers	x	x	x	x	x								x	x		x			
Governments												x	x						
Other answers added by the scheme	(1)	(2)								(3)			(4)						
List typical sponsors and risk owners																			
Service Providers			x				x	x	x				x	x	(14)				
Product vendors		x	x				x	x	x		x		x	x		x			
Integrators			x				x	x	x					x					
Operators		x	x				x	x	x					x					
Evaluation Laboratory																			
Certification Body				x															
Government organisations		x									x	x							
Other answers added by the scheme		(5)					(6)	(6)	(6)	(7)			(8)						
List of end users																			
End-Customers	x	x	x	x	x	x	x	x	x		x		x		x				
Service Providers	x	x	x	x	x	x	x	x	x		x		x	x		x			
Integrators		x	x	x	x	x	x	x	x				x	x		x			
Government organisations	x	x		x								x	x						
Telco operators, banking, energy, etc.		x	x		x	x	x	x	x				x						
Other answers added by the scheme	(1)	(9)					(10)	(10)	(10)	(11)			(12)						

Other answers:

- (1) Governmental organizations. Can vary from top government (SSC-IT) to local governmental bodies. Also, organizations involved in NL vital sectors or industry. Also, vendors / developers are welcome. This scheme is open to whoever pays for the assessment.
- (2) French Administration (due to French general security framework, aka RGS), Undisclosed private risk owners: energy, banking, etc.

- (3) The scheme is comprehensive and voluntary and can be applied broadly. It is especially attractive to start-ups and traditional manufacturers that rely on embedded systems which are now introducing connectivity to enhance those products or create new services.
- (4) Could be anybody.
- (5) Public risk owners such as ANSSI/SGDSN, ANTS. Private risk owners such as Orange, GIE SESAME VITALE.
- (6) Banks, Insurers, Real estate developers, Any asset owner, Any network connectivity provider, Any service provider, Any buyer, Any manufacturer
- (7) IOT solution vendors and their customers throughout a supply chain. The power of the scheme is that it is risk based, and can be used at component, service and product level.
- (8) Any form of platform developer.
- (9) The direct users are the developers and sponsors. Sponsors can be either:
  - a. French Administration or Private risk owners (who need certification for procurement reasons),
  - b. Product vendors themselves (who need certification for marketing reasons)
- (10) Retailers / distributors, Tech giants, Telco operators, Consumers, Building owners / operators, Factory owners / operators, Installers / architects / designers, Utilities"
- (11) Those that have a need to demonstrate IoT cybersecurity assurance for their business. This covers most IOT product or solution vendor. It also includes those providing security services for vendors such as IoT security consultants and evaluation laboratories.
- (12) Could be anybody
- (13) The scheme BSI Base Certification is currently still in market entry. Therefore, there is no group available that actually insists on used certificates issued by the scheme.
- (14) No assurance scheme.

## 2.3. Operational Description and Governance of the Scheme

### (Q4, Q6, Q7, Q8, Q9, Q10, Q11, Q31, Q32, Q33, Q34)

Table 4: Scheme details (Q4, Q6, Q7, Q8, Q9)

Scheme	Scheme documentation owner	Certificate issuer	Number of issued certificates	Location of published certificates	Certification fees
BSPA (NLNCSA)	AIVD/NLNCSA	(3)	N/A, (3)	Not yet available	(6)
CSPN (ANSSI)	ANSSI	ANSSI	>100	<a href="https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/">https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/</a>	Free
Eurosmart IoTSCS	Eurosmart	Accredited CAB-R	0, pilot phase	Eurosmart and CAB websites	(6, 7), 2k-5k EUR
LINCE	CCN and SSB	CCN	12	Not answered	Free
PSA L1	PSA	ARM	26	<a href="https://www.psacertified.org/certified-products/">https://www.psacertified.org/certified-products/</a>	(6, 7)
PSA L2	PSA	ARM	0, pilot is planned		(6, 7)

Scheme	Scheme documentation owner	Certificate issuer	Number of issued certificates	Location of published certificates	Certification fees
UL IoT Security Rating	UL	UL	0, pilot phase	Under development	(6, 7)
UL 2900	(1)	(1)	>0, unknown	<a href="https://iq.ulprospector.com/info/">https://iq.ulprospector.com/info/</a>	(6, 7)
UL IEC 62443	(1)	(1)	>0, unknown		(6, 7)
IOTSF	IoTSF	N/A, (4)	N/A, (4)	N/A, (4)	Free
BSI Base Certification	BSI	BSI	0, pilot phase	Scheme web page	4k EUR
SOG-IS for IoT	SOG-IS	CC scheme bodies	> 10	Scheme web page	Nation specific
SESIP	TrustCB, (2)	TrustCB, (2)	3	<a href="https://trustcb.com/iot/sesip/sesip-certificates/">https://trustcb.com/iot/sesip/sesip-certificates/</a>	(6), 3k – 20k EUR
TÜVIT-SQ	TÜVIT	TÜVIT	10 products, 23 systems	<a href="https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-installationen/">https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-installationen/</a> <a href="https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-produkten/">https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-produkten/</a>	(7,8) 5k-10k EUR
ETSI	ETSI is not a certification scheme.				
GP TEE	GP and GP TEE technical committee	GP secretariat	3 certificates are published on the web page, more certificates not published have been indicated.	<a href="https://globalplatform.org/certified-products/?filter-certification-type=security">https://globalplatform.org/certified-products/?filter-certification-type=security</a>	For GP members: 5,5k EUR / 12k EUR For others: 11k EUR / 17k EUR (9)
GP SE					
GSMA					
CPA					

## Other answers:

- (1) ANSI or IECCE accredited organizations including UL.
- (2) SESIP is currently in a process to become an open standard. Currently TrustCB is the CB responsible.
- (3) There is no delivery of certificates. A deployment advisory with a Statement of Conformity (SoC) is issued. A Statement of Conformity (SoC) is part of the Deployment Advisory (DA) and is only valid if the recommendations and obligations in the DA are being followed.
- (4) Currently in self-certification state.
- (5) Until June 2019, the scheme issued more than 100 certificates (295 evaluations led to 141 certifications).
- (6) Was not answered.
- (7) Depends on the product complexity and/or addressed evaluation level.
- (8) Price list is private.
- (9) The price list is public: [http://globalplatform.org/wp-content/uploads/2019/02/Security-Certification-Fees\\_02082019.pdf](http://globalplatform.org/wp-content/uploads/2019/02/Security-Certification-Fees_02082019.pdf)

Table 5: Scheme maintenance (Q10, Q11)

Scheme	Scheme documentation is maintained by a group of experts	Certificate lifetime	Vulnerability management after certificate has been issued?
BSPA (NLNCSA)	x (NLNCSA)	Unlimited	Yes
CSPN (ANSSI)	x (ANSSI)	3 years	No
Eurosmart IoTSCS	Yes	Not yet defined	Yes
LINCE	Yes (CCN and SSB)	5 years	Yes
PSA L1	Yes	Unlimited	No
PSA L2	Yes	Unlimited	No
UL IoT Security Rating	Yes	1 year	Yes, customers are required to adhere to a vulnerability management process, which may or may not be facilitated by UL. It depends on issues found, their risk-level and how they are mitigated.
UL 2900	Yes	1 year	
UL IEC 62443	Yes	1 year	
IOTSF	Yes (IoTSE)	Unlimited	Yes. The scheme has supporting documentation (a best practice guide) and the recommended process follows ISO/IEC 29147
BSI Base Certification	Under definition		
SOG-IS for IoT	Yes	Domain specific	Nation-specific
SESIP	Yes	2 years	Yes. Certificates can be withdrawn
TÜVIT-SQ	Yes	2 years	Yes, for highest evaluation level SEAL5)
ETSI	ETSI is not a certification scheme.		
GP TEE	Yes	3 years	Regular expert meeting to update attack methodology and certified products should review new attacks. Based on that, certificates can be withdrawn and a reevaluation has to be conducted.
GP SE			
GSMA			
CPA			

Table 6: Risk Analysis and Management (Q31, Q32, Q33, Q34)

	BSPA (NLNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Does the scheme include a risk management process?																			
Yes, during the life cycle of the evaluation		x	x				x	x	x	x	x	x	x	x					
Yes, after the certificate issuance			x				x	x	x							x			
No	x			x	x	x									x				
Is the evaluation based on a risk analysis prior to the evaluation to determine the evaluation level required?																			
Yes, to be performed by the developer or vendor										x									
Yes, to be performed in collaboration between developer and evaluator			x																
No, it is not based on a risk analysis	(1)	x		x	x	x					x	x	x	x	x	x			
Reuse evaluation and audit results from other certification schemes (e.g. CC, EMVCo, FIPS, GP, GSMA)																			
Yes	x	CC	x									CC	(2)	(3)		(4)			
No				x	x	x					x				(5)				

Other answers:

- (1) Developer choice, customer choice
- (2) CC (SOG-IS) for SESIP5; ARM PSA, FIPS140, ICA, and others such as GlobalPlatform
- (3) CC and FIPS 140-2
- (4) SOG-IS and EMVCo
- (5) No answer provided

## 2.4. Products Evaluated by the Scheme (Q22, Q23, Q24)

Table 7: Mapping between schemes and products (Q22, Q23, Q24)

	BSPA (NLNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Product types																			
Secure elements (SE)		x										x	x						
Multi-application processors		x	x		x	x						x	x			x			
System on Chip (SoC)		x	x		x	x						x	x	x		x			
xG baseband hardware/software for mobile communication		x											x						
Sigfox baseband hardware/software for IoT services		x	x									x	x						
Sensors		x					x	x	x		x	x	x			x			
Hardware Security Modules (HSM)		x										x	x						
Network devices like routers, switches, etc.		x		x			x	x	x		x	x	x	x		x			
Trusted Platform Module (TPM)		x										x	x	x					
Security ICs (hardware only)		x										x	x		(8)	x			
Security ICs including embedded software like operating systems and applications		x			x	x	x	x	x			x	x			x			
Software applications running on SOC or SE or any mobile environment		x		x			x	x	x		x	x	x	x		x			
Software applications running Cloud servers		x		x			x	x	x		x	x		x					
Database servers		x		x			x	x	x		x	x		x					
Qualified Electronic Signature Creation Device (QSCD)		x										x							
Other answers added by the scheme	(1)			(2)			(3)	(3)	(3)	(4)									
General purpose (can be applied for any type of products)		x	x	x								x	x	x					
Product level																			
System level	x	x					x	x	x	x		x		(7)					
Component level	x	x	x	x	x	x	x	x	x	x	x		x	x	(8)	x			
Process/enterprise level									x					x					

	BSPA (NUNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜViT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Support of Composition?																			
Yes	x	x	x	-	x	-	(5)	(5)	(5)	x	(5)	(6)	x	x	(8)	x			
No	-	-	-	x	-	X				-		-	-						

Other answers:

- (1) Government, Access Control, Network Security, Network filtering, detection and response, secure messaging, Media and file security
- (2) IoT device
- (3) Consumer products, commercial products, industrial/OT products and systems, and medical devices
- (4) The scheme is best applied at the product level however it is also applicable at the component (hardware and software) level too.
- (5) No answer given / state unknown.
- (6) A composite process is defined for smartcards only.
- (7) The scheme TÜViT-SQ allows a certification of an IoT device including a corresponding backend (cloud server).
- (8) ETSI is not an assurance scheme.



## 2.5. Evaluation Methodology/-ies used by each Scheme

### 2.5.1. Evaluation Labs (Q18, Q19, Q20, Q21)

Table 8: Evaluation Labs (Q18, Q19, Q20, Q21)

	BSPA (NLNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC G2443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA	
Security Evaluation																				
No security evaluation										(1)					x					
Self-assessment					x															
Independent security evaluation by an approved lab	x	x	x	x		x	x	x	x			x	x	x	x		x			
Approved Laboratories																				
The scheme already has approved security labs	x	x		x	x	x	x	x	x	(8)	(2)	(3)	x	x	(8)	x				
Number of approved laboratories	3	10		2	4	4	(4)	(4)	(4)	(8)		(6)	1	1	(8)	7				
Accreditation in progress			x	5									7							
Approval process of the evaluation laboratories																				
No specific approval process					x	x				x				x	x					
Laboratories already approved by other schemes are accepted			x	x			(4)	(4)	(4)							(7)				
Specific approval process	(5)	x	x	x							x	x	ISO17025							
Expertise required for the evaluation labs																				
Software only					x															
Hardware and/or software	x	x	x	x		x	(4)	(4)	(4)	x	x	x	x	x	(4)	x				
Technology used by the evaluated products	x	x	x	x						x	x	x	x							

Other answers:

- (1) Not explicitly however sub-elements of a product may rely on independent lab certificates – this is for the user to determine and is guided by the application use case.
- (2) Pilot phase.
- (3) Accreditation by national certification bodies.
- (4) No answer provided.

- (5) The scheme implements a licensing process. A lab has to apply to become licensed. A lab makes a request to be licensed on certain categories, they provide evidences that prove experience, this is assessed and audit is performed by NLNCSA. With doing a good first / trial assessment the lab is licensed for products of a certain category. The next assessment is performed with NLNCSA doing less oversight.
- (6) Nation Specific
- (7) Delta based on SOG-IS PCI or EMVCo.
- (8) No labs available.

## 2.5.2. Evaluation Process (Q12, Q13, Q14, Q15, Q16, Q17)

Table 9: Evaluation Process (Q12, Q13)

Scheme	Support of Maintenance / continuous assurance procedures	Supported Evaluation Levels	Evaluation Level (short description)
BSPA (NLNCSA)	Yes, delta assessments	Only one level	Baseline: Basic evaluation level.
CSPN (ANSSI)	Yes	Only one level	High evaluation level: Equivalent to CC AVA_VAN.3.
Eurosmart IoTSCS	Yes	Only one level	Substantial evaluation level.
LINCE	Yes	Basic, Basic + MEC, Basic + MCF, Basic + MC + MCF	Basic corresponds to the LINCE evaluation which can be augmented with a cryptographic evaluation (+ MEC), a source code review (+ MCF), or both (+MEC + MCF).
PSA L1	No	PSAcertified L1, L2, L3	
PSA L2	No		
UL IoT Security Rating	(1)	Bronze, Silver, Gold, Platinum, Diamond	The levels range from a baseline evaluation (Bronze) to a more comprehensive security capabilities.
UL 2900	(1)		For UL, levels are defined in sub-standards.
UL IEC 62443	(1)		The scheme defines security and maturity levels
IOTSF	(2)	(3)	(3)
BSI Base Certification	Yes	Only one level	Substantial evaluation level.
SOG-IS for IoT	Yes	EAL1 to EAL7 with augmentations	EAL1 is a basic evaluation level with only a few formal requirements. EAL7 is the highest assurance level which requires the usage of formal proofs and representation (for instance).
SESIP	Yes	SESIP1 to SESIP 5	SESIP1 corresponds to a developer statement; SESIP5 is equivalent to a full CC EAL4+ evaluation.
TÜVIT-SQ	No	SEAL1 to SEAL5	SEAL1 is the lowest evaluation level for which the security requirements need to be specified. No penetration testing is done. SEAL2 can be considered as a consulting process, as in addition to SEAL1, penetration testing is performed. A certificate is issued for SEAL3+. SEAL5 includes change management.
ETSI	ETSI is not an assurance scheme.		
GP TEE	Not yet. Continuous assurance will be introduced in the SE scheme in 2020 and then ported to TEE.	Only one evaluation level.	The GP TEE certification scheme aims for a moderate evaluation level.
GP SE			
GSMA			
CPA			

Other answers:

- (1) Depends on certification validity and any re-testing/re-certification needs based on surveillance and vulnerability management processes.
- (2) The scheme is a blend of assurance and certification assessments – some are one time, others require maintenance.
- (3) The scheme has general applicability as it is risk-based. The user is guided to identify a compliance class and the security requirements follow the level of the chosen compliance class. The basic mechanism is in place and more materials are being produced to help users select a compliance class to self-certify against.

Table 10: Evaluation requirements (Q14, Q16)

	BSPA (NINCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Documentation Requirements																			
No documentation requirements															x				
High-level information		x	x		x						x								
Complete information including low-level design information		(3)	x	(5)		x	(13)	x	x		(3)	(9)	(11)	(8)		x			
Source code		(14)	(14)			x		x	x		(3)	(9)							
Scheme-specific information	(1)	x				x				(12)	(3)	(10)		(9)					
Functional Testing Requirements																			
No functional testing required											x	x		x	x				
Required for the developer	(2)		x	x	x	x	(2)	(2)	(2)	x			x			(19)			
Required for the evaluator		x		x									(6)						
Penetration Testing Requirements																			
No penetration testing required					x					(15)					x				
Required for the evaluator	x	x	x	x		x	(2)	(2)	(2)		x	x	(7)			x			
Development and Production Sites																			
No site security requirements (The Scheme recognizes third party audits when applicable)	x	x	(4)	x	x	x	x	x	(17)	x	x	(16)	(8)		x				

	BSPA (NLNC5A)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Site audits for all development sites																x			
Site audits for all production sites																			

Other answers:

- (1) The lab has to use templates provided by the certifier (ETR and DA (Deployment Advisory)).
- (2) No answer provided.
- (3) For crypto only.
- (4) Self-assessment of site audits. Required information are filled within the questionnaire by the developer and there is no audit by the Lab.
- (5) High-level documentation for the evaluation level Basic; MEC required low-level documentation; MCF requires low-level documentation and source code.
- (6) For SESIP2 and higher.
- (7) Only in case of SESIP1, no penetration testing is performed.
- (8) For SESIP1 to SESIP3: no site security requirements; for SESIP4: Secure development practices have to be shown but not necessarily in a site audit; for SESIP5: a lab has to audit all production and development sites.
- (9) For EAL3 and higher.
- (10) For EAL2 and higher: Security Architecture and test documentation; for EAL6 and higher: formal security policy model.
- (11) SESIP1: only a self-declaration is required; SESIP2: high-level documentation; SESIP3/4: source code; SESIP5: Equals full EAL4+.
- (12) Evaluation file is constructed by the user – A questionnaire is provided to support the scheme and provides all necessary links to supporting documentation within the users organization.
- (13) Bronze / Silver: high-level documentation; Gold / Platinum / Diamond: low-level documentation; Diamond: source code.
- (14) For critical parts only.
- (15) The scheme may include penetration testing however this is self-directed by the user and the evidence of the tests can be included in the evaluation file.
- (16) EAL1/2: No site security requirements; EAL3 and higher: all development and production sites have to be audited; Audit recognition within SOG-IS.
- (17) Depends on which sub-standard is applied.

(18)SEAL1/2: Security Requirements need to be defined; SEAL3: Architectural design required; SEAL4: Source code review; SEAL5: Change management.

(19)The lab has to perform functional tests. However, if a functional compliance is available, the developer can use a specific test suite. This reduces the efforts for the evaluation lab.

This is how the different schemes support patching of certified products **(Q15)**:

- BSPA (NLNCSA) supports delta evaluations.
- CSPN (ANSSI): The scheme allows the evaluation of secure patching mechanisms, but it does not extend the certificate validity to patched products.
- BSI Base Certification: Not supported. For changed/updated products a re-evaluation is required.
- The schemes Eurosmart IoTSCS, LINCE, PSA L1, PSA L2, UL IoT Security Rating, UL 2900, UL IEC 62443, and IoTSF support patching without further restrictions.
- The scheme SOG-IS for IoT supports 'Assurance Continuity'. It allows the evaluation of secure patching mechanisms, but it does not extend the certificate validity to patched products.
- The scheme TÜVIT-SQ certifies a fixed version of the product. However, in case of SEAL5, the evaluators check the change management processes of the developer to provide further assurance that updates are done in a reasonable and secure way.
- The scheme GP TEE supports patching. No further description has been provided.

**Table 11: Supporting documents of the schemes (Q17)**

Scheme	Questionnaire	Security Profile / Protection Profile	Templates for Developer Documents	Guidance for Developers	Guidance for Evaluators	Mandatory Technical Specifications / Standards that need to be applied
BSPA (NLNCSA)	Not available.	Not available.	Not available.	Not available.	ETR template and DA (1)	None
CSPN (ANSSI)	Not available.	Available.	Template for Security Target.	Not available.	Available.	RGS guidance; CEM / ISO 18045 (2)
Eurosmart IoTSCS	Available.	Available.	Not available.	Not available.	Not available.	None.
LINCE	Not available.	Available.	Not available.	Available.	Available.	(3)
PSA L1	Available.	Not available.	Not available.	Available.	Not available.	(3)
PSA L2	Available.	Available.	Not available.	Available.	Available.	(3)
UL IoT Security Rating	(4)	(4)	(4)	(4)	(4)	(4)
UL 2900	(4)	(4)	(4)	(4)	(4)	(4)
UL IEC 62443	(4)	(4)	(4)	(4)	(4)	(4)
IoTSCS	Available.	Not available.	Not available.	Not available.	Not available.	None.
BSI Base Certification	Not available.	Not available.	Not available.	AIS B1 to B5	AIS B1 to B5	None.
SOG-IS for IoT	Not available.	Available.	Available	Available.	Available.	Product-specific.
SESIIP	Not available.	Available.	Template for Security Target.	Not available.	Product-specific.	CC, ISO17025
TÜVIT-SQ	Not available.	Not available.	Not available.	Not available.	Not available.	Not available.
ETSI	Not available.	Available.	Not available.	Not available.	Not available.	Not available.

Scheme	Questionnaire	Security Profile / Protection Profile	Templates for Developer Documents	Guidance for Developers	Guidance for Evaluators	Mandatory Technical Specifications / Standards that need to be applied
GP TEE	Not available.	Available.	Available.	Not available.	Available.	TEE protection profile, TEE specific APIs
GP SE						
GSMA						
CPA						

Other answers:

- (1) The developer should deliver a product that is able to resist the Baseline level (no state actors etc.). The scheme uses a black box approach. A baseline assessment is a job for a lab to black box pentest / break the claimed security functions in any way they can in 25 man days. The lab has to convince our experts in the technical report they have been using their time wisely making the right and expected choices given the nature of the product and the current knowledge about the used technologies etc. The lab should do what a hacker would do. Anything that's available or can be found should be used to break the product. For example, if code for an attack is only, it should be used.
- (2) In addition, application notes are available that are public or restricted to specific sponsors and evaluators.
- (3) Mandatory documentation has to be used. However, no details have been provided.
- (4) No answer provided.

### 2.5.3. Testing Process (Q25, Q26, Q27, Q28, Q29, Q30)

Table 12: Compliance overview (Q25, Q26, Q27, Q28, Q29, Q30)

	BSPA (NLNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Definition and maintenance of the attack catalog																			
No attack catalog	(1)			x						x	x				x				
Maintained by a group of experts		x			x	x	x	x	x			x		x		x			
Maintained by the scheme		x																	
Definition and maintenance processes are not yet defined			x																
Other												(2)							

	BSPA (NINCSA)	CSPN (ANSSI)	IoTCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC G2443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA		
Collection of information by the security lab																					
Black box analysis, no inputs required	x										x		(7)	(28)	(37)						
via workshops with the developer				x									(6)								
Set of documents (examples: Questionnaire including required evidences, Security Target, etc.)			x	x	x	x	x	x	x	x	(4)	x	(5)	(29)		x					
Other		(3)																			
Balance between functional tests, penetration tests and document review																					
No security evaluation					(9)		(10)	(10)	(10)	(9)			(7)		x						
Functional tests [%]		40	15	24		0					0	0	0			30					
Penetration tests [%]		40	30	64		90					92	30	75	80		50					
Document review [%]		20	30	12		10					8	70	25	20		20					
Source code review [%]			15			(10)								(30)		(34)					
Other	(8)																				
Evaluation workload																					
Full Evaluation	(11)	(12)	(14)	(15)	(16)	(17)	(10)				(18)	(19)	(20)	(31)	(37)	(35)					
Re-Evaluation or Delta	(10)													-		-					
Approach used for penetration tests																					
No security evaluation					(9)		(10)	(10)	(10)	(9)			(7)	(32)	x						
Black-box testing	x	x	x	(22)							x		(7)								
Gray-box testing	(21)	(21)	x																		
White-box testing		(4)	x	(23)		x					(4)	x	(24)			x			x		
Supported crypto algorithms																					
No requirements regarding implemented crypto algorithms	x						(10)	(10)	(10)			(25)									
Implementation of state-of-the-art cryptographic algorithms and key sizes from national security agencies (such NIST for U.S., BSI for Germany, CESG for U.K., ANSSI for France), SOG-IS or from academia.		x	x		x	x					x	x		x	x	x	(36)				

	BSPA (NUNCSA)	CSPN (ANSSI)	IoTSCS	LINCE	PSA1	PSA2	UL IoT Security Rating	UL 2900	UL IEC 62443	IOTSF	BSI Base Certification	SOG-IS IoT	SESIP	TÜVIT-SQ	ETSI	GP TEE	GP SE	GSMA	CPA
Proprietary cryptographic algorithms or customization of standard cryptographic algorithms				x									x						
Verification of implementation of crypto algorithms																			
No verification							(1)	(1)	(1)	(26)					x				
Only documentary verification					x														
Verification by functional tests only				x									x						
Verification by documentation, functional tests and source code review		x	x			x					x					x			
Verification by penetration tests only																			
Other	(25)											(27)		(33)					

## Other answers:

- (1) We do a review by experts that will assess the lab technical report. When our experts feel the lab did not consider what they would expect (like a specific attack) we will question the lab.)
- (2) Existing attack catalogs are reused
- (3) Mostly black-box but: Cryptography requires dedicated and detailed documentation from the dev and specific contexts may mandate documentation (will typically be mandated in application notes)
- (4) For Crypto only
- (5) For SESIP5
- (6) For SESIP3/4
- (7) SESIP1: no evaluation; SESIP2: black box
- (8) The lab may convince us in the technical report why they made the right choice in approach on the specific product.
- (9) Self-assessment
- (10) No answer provided
- (11) 25-man days
- (12) 25 work days + 10 days for the crypto



- (14) 2 weeks
- (15) 8 weeks
- (16) One week
- (17) 2 to 3 months
- (18) 40-50-man days
- (19) 9-12 months
- (20) SESIP1: 3-5 days, SESIP5: 3-5 months
- (21) if code is available
- (22) Basic
- (23) MCF
- (24) SESIP 3, 4 and 5
- (25) Correct implementation should be assessed in a smart way given the limited amount of time the lab has, with the goal to find mistakes to break the product.
- (26) User determined
- (27) code review, security testing / pentest
- (28) For SEAL2 only
- (29) For SEAL3+
- (30) For SEAL4+ only
- (31) 6 months
- (32) SEAL2: Black-box testing; SEAL3+: White-box testing
- (33) SEAL4+ requires a source code review. In this case, the correct implementation of standards can be verified in case a corresponding security requirement is defined.
- (34) Source code review is included in the remaining topics but has not been answered separately.
- (35) 100 days
- (36) GP TEE defines which algorithms are accepted. This list is not public.
- (37) No security evaluation

## 2.6. Compliance Level with Art. 54 of the Cyber Security Act (Q35)

Table 13: Compliance overview (Q35)

Scheme	Recognition by the EU Cyber Security Act	Is the scheme already compliant?
BSPA (NLNCSA)	To be determined.	No answer provided.
CSPN (ANSSI)	Recognition is intended.	Partially.
Eurosmart IoTSCS	Recognition is intended.	Yes (except (u))
LINCE	Recognition is intended.	Partially
PSA L1	Recognition is not intended.	Partially

Scheme	Recognition by the EU Cyber Security Act	Is the scheme already compliant?
PSA L2	Recognition is not intended.	Partially
UL IoT Security Rating	Recognition is intended.	No answer provided.
UL 2900	Recognition is intended.	No answer provided.
UL IEC 62443	Recognition is intended.	No answer provided.
IOTSF	Recognition is intended.	Partially
BSI Base Certification	Recognition is intended.	No answer provided.
SOG-IS for IoT	Recognition is intended.	No answer provided.
SESIP	Recognition is intended.	Partially (list provided)
TÜVIT-SQ	To be determined.	No answer provided.
ETSI	Recognition is intended.	Partially.
GP TEE	Recognition is intended.	No answer provided.
GP SE		
GSMA		
CPA		

Table 14: Compliance details

Compliance mapping		
	Eurosmart IoTSCS	SESIP
(a) subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services	X	
(b) a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme	X	
(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II of Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme	X	
(d) where applicable, one or more assurance levels	X	
(e) an indication of whether conformity self-assessment of conformity is permitted under the scheme	X	
(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements	X	X
(g) The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 51 are achieved	X	X
(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant	X	X
(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used	X	X
(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements	X	X
(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification	X	X
(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme	X	X

Compliance mapping		
	Eurosmart IoTSCS	SESIP
(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with	X	X
(n) where applicable, rules concerning the retention of records by conformity assessment bodies	X	X
(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels	X	X
(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued	X	-
(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes	X	-
(r) maximum period of validity of European cybersecurity certificates issued under the scheme	X	X
(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme	X	X
(t) conditions for the mutual recognition of certification schemes with third countries	X	(1)
(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59.	-	-
(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.	X	-

Note:

(1) Not answered.

### 3. References

**ETSI** Cyber Security for Consumer Internet of Things, ETSI TS 103 645, Version 1.1.1, 2019-02.  
[https://www.etsi.org/deliver/etsi\\_ts/103600\\_103699/103645/01.01.01\\_60/ts\\_103645v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf)

**BSI Base Certification** (Not yet published).

**SESIP** Security Evaluation Standard for IoT Platforms, Version 1.3, NXP Semiconductors N.V. (see <https://www.trustcb.com/iot/sesip/>)

**SOG-IS (CC)** see <https://www.sogis.eu/>  
 Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001, Part 2: Security functional components, Version 3.1, Revision

5, April 2017, CCMB-2017-04-002, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003.

Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004.

<b>TÜViT-SQ</b>	(Not published).
<b>BSPA</b>	(Not published).
<b>CSPN</b>	(see <a href="https://www.ssi.gouv.fr/administration/produits-certifies/cspn/">https://www.ssi.gouv.fr/administration/produits-certifies/cspn/</a> )
<b>Eurosmart IoTSCS</b>	(see <a href="https://www.eurosmart.com/eurosmart-iot-certification-scheme/">https://www.eurosmart.com/eurosmart-iot-certification-scheme/</a> )
<b>GSMA</b>	(see <a href="https://www.gsma.com/iot/iot-security-assessment/">https://www.gsma.com/iot/iot-security-assessment/</a> )
<b>GP TEE</b>	TEE System Architecture, GlobalPlatform TEE Internal API Specification, GlobalPlatform TEE Client API Specification, GlobalPlatform GlobalPlatform Device Committee, TEE Protection Profile <a href="https://globalplatform.org/specs-library/tee-protection-profile-v1-2-1/">https://globalplatform.org/specs-library/tee-protection-profile-v1-2-1/</a>
<b>GP SE</b>	(see <a href="https://globalplatform.org/certifications/security-certification/">https://globalplatform.org/certifications/security-certification/</a> )
<b>IoTSEF</b>	(see <a href="https://www.iotsecurityfoundation.org/best-practice-guidelines/">https://www.iotsecurityfoundation.org/best-practice-guidelines/</a> )
<b>LINCE</b>	(Not published).
<b>PSA</b>	(see <a href="https://www.psacertified.org">https://www.psacertified.org</a> )
<b>UL IoT Security Rating</b>	(Not yet published).
<b>UL 2900</b>	(see <a href="https://iq.ulprospector.com/info/">https://iq.ulprospector.com/info/</a> )
<b>UL IEC 62443</b>	(see <a href="https://iq.ulprospector.com/info/">https://iq.ulprospector.com/info/</a> )

**CPA**

(see <https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa>)

Eurosmart members - restricted distribution

## 4. Revision History

Version	Changes / Application Note	Author
0.1	Initial Version	TÜViT
0.2	Intermediate Version	IOTR
0.3	Added scheme TÜViT Security Qualification	TÜViT
0.4 to 0.6	Consistency with tables, complementary information (explanatory notes), multiple responses merge ; introduction	IOTR
0.7	Added schemes ETSI and GP TEE. Added reference list.	TÜViT
1.0	Final Version for Eurosmart review	IOTR & TÜViT
1.1	Final Version to be shared with Eurosmart Board members	IOTR & TÜViT